

TROUBLESHOOTING

After reading this chapter and completing the exercises, you will be able to:

- ◆ Develop your own problem-solving strategy
- ◆ Use the Event Viewer to locate and diagnose problems
- ◆ Troubleshoot configuration, security, connectivity, and network printing problems
- ◆ Troubleshoot boot problems, using a variety of tools including the emergency repair disk, safe mode, and the recovery console
- ◆ Back up and restore system state data

Troubleshooting is a basic part of working with computers and is closely linked to the skills you have learned for monitoring and tuning. Sometimes problems can be prevented by monitoring, but at other times problems strike without warning, such as when a server suddenly will not boot. In nearly all cases, troubleshooting a server problem is accompanied by a sense of urgency, because users depend on servers. At the same time, the more you troubleshoot, the more you develop solid troubleshooting skills and learn about servers and networks.

In this chapter, you learn troubleshooting skills to give you confidence in many situations. You learn how to resolve server and network connectivity problems, configuration problems, printing problems, boot problems, and many others. Along the way, you learn to use vital troubleshooting tools such as the Event Viewer, the System Security and Analysis tool, safe mode, the emergency repair disk, and the recovery console.

DEVELOPING A PROBLEM-SOLVING STRATEGY

The best approach to solving server and network problems is to develop troubleshooting strategies. Three general strategies are:

- Understanding how a server and the network interact
- Training your users to help you solve problems
- Knowing the business processes of your organization

Understanding How Servers and the Network Interact

There are many steps you can take to better understand the environment in which a server operates. Many server and network administrators create a diagram of the entire network and update the diagram each time an aspect of the network changes. The network diagram should include the following elements:

- Servers
- Host computers
- Workstations and network printers (unless the network is too large to include these)
- Network devices
- Telecommunications links
- Remote links
- Building locations
- Cable link types, such as copper or fiber, and link speeds

A server does not exist in a vacuum, but instead is a member of a larger community of networked workstations and their users. Gathering benchmarks, as discussed in Chapters 14 and 15, helps you understand your server and how its network context affects it. For example, slow server performance can look like a network problem, and slow network performance can look like a server problem. The more you know about the server's network context, the faster you will be able to resolve a problem such as slow server performance.

Training Users to Help

Another valuable strategy is to train network users to be your partners in reporting problems. If you encourage users to be troubleshooting allies, they are more likely to feel they can take action to deal with a problem, rather than wait impatiently for you to detect and solve it. When you train users to gather information and report it to you, they become troubleshooting partners who can advance you several steps toward the solution. The following are some actions you can train users to take to help you and themselves. For example, they should:

- Save their work at the first sign of a problem
- Carefully record information about a problem, such as the exact wording of error messages, the impact on their workstation, and the impact on others working nearby

- Report any protocol information, such as error messages about a protocol or an address
- Quickly report a problem by telephone, or by voice mail if you cannot be reached immediately
- Avoid sending e-mail about urgent problems

Knowing the Business Processes of Your Organization

Your knowledge of how your organization works is another tool for solving problems. For example, assume you are the server administrator at a college library, and the catalog server is reported to be slow just before 1:00 p.m. and 6:00 p.m. Your knowledge of library activities might indicate that the network or a server is slow because large numbers of students are checking out books just before going to afternoon classes or to the dorms for dinner. In another case, you might work at a business where network problems occur each morning when the company president downloads a huge database or runs several giant reports. Your understanding of how people work in your organization can help you take the appropriate steps for finding solutions, such as tuning a server.

Solving Problems Step by Step

Equipped with knowledge of your network context, trained users, and an understanding of your organization, you can use the following step-by-step technique to solve network problems.

1. *Get as much information as possible about the problem.* If the problem is reported by a network user, listen carefully to his or her description. Even if he or she does not use the right terminology, the information is still valuable. Part of your challenge is to ask the right questions to get as much information as possible.
2. *Record the error message at the time it appears or when a user reports it to you.* This is an obvious but sometimes overlooked step. If you try to recall the message from memory, you may lose some important information. For example, the error “Network not responding” can lead you to a different set of troubleshooting steps than the message “Network timeout error.” The first message might signal a damaged NIC, whereas the second message could mean that a database server is overloaded and the application is waiting to obtain data.
3. *Start with simple solutions.* Often the solution to a problem is as simple as connecting a cable or power cord.
4. *Determine if anyone else is experiencing the problem.* For example, several people may report they cannot load a word-processing software package. This may be due to a problem at the server they use to load the software. If only one person is experiencing this problem, it may point to trouble on her or his workstation.
5. *Check to see if any recent alerts have been sent to your account.* If you have set up alerts, check to determine if any have been sent warning you of a problem.

6. *Check the event logs.* Regularly check the Windows 2000 Server event logs (discussed later in this chapter) for signs of a problem.
7. *Use System Monitor performance logs and Network Monitor filtering.* Perfect your skills at using System Monitor performance logs and Network Monitor filters to trap detailed information about a problem (see Chapter 14 and 15).
8. *Check for power interruptions.* Power problems are a common source of server and network difficulties. Even though the server is on a UPS, its network connection can still be a source of problems, because the network cable can carry current to the server's NIC during a lightning storm, or because of a major power-related problem.

Tracking Problems and Solutions

One effective troubleshooting tool is to keep a log of all network problems and their solutions. Some server administrators log problems in a database created for that purpose. Others build problem logging into help desk systems maintained by their organization. A help desk system is application software designed to maintain information on computer systems, user questions, problem solutions, and other information that members of the organization can reference.

The advantage of tracking problems is that you soon accumulate a wealth of information on solutions. For example, to jog your memory about a solution, you can look up how you handled a similar problem six months ago. The log of problems also can be used as a teaching tool and reference for other computer support staff. Problems that show up repeatedly in the log may indicate that special attention is needed, such as replacing a server that experiences frequent hardware problems.

Using the Run As Option

There are times when you are troubleshooting Windows 2000 Server or a Windows 2000 Professional workstation when someone else is logged on who does not have the full privileges needed to work on the problem, particularly when Administrator privileges are required. Further, if he or she is in the middle of work, it is disruptive to have to log off so that you can log on as Administrator to fix the problem. Windows 2000 comes with the **Run as** option, which enables you to temporarily access a program and other Windows 2000 utilities without logging off the current user. In most situations, to use the *Run as* option, you right-click the program and click *Run as* on the shortcut menu. For example, to run the Computer Management tool so that you can start a particular service as Administrator, you would click Start, point to Programs, point to Administrative Tools, right-click Computer Management, click Run as, click *Run the program as the following user*, and enter Administrator, the Administrator account password, and the domain (if the Active Directory is in use).



Alternatively, you can execute *runas* from the Command Prompt window. For example, to access the Command Prompt window as Administrator in the domain TheFirm.com, when another account is already logged on, you would open the Command Prompt window, type `runas/user:thefirm.com\administrator cmd`, press Enter, enter the Administrator account's password, and press Enter.



The Run as option will only work if the RunAs service is already started. If it is not, right-click My Computer, click Manage, double-click Services and Applications, click Services, double-click the RunAs Service, and click Start. As you have probably realized, the Run as option is referred to in different ways: *Run* as in the shortcut menu, *runas* in the Command Prompt window, and *RunAs* for the service name.

USING THE EVENT VIEWER TO TROUBLESHOOT PROBLEMS

A good place to begin your diagnosis of a server problem is the event logs displayed in the Event Viewer (see Figure 16-1). There are three principal **event logs** that contain a record of all types of server events: system, security, and application. Also, there are event logs for services that you may have installed, such as the Directory Service, DNS Service, and File Replication Service logs.

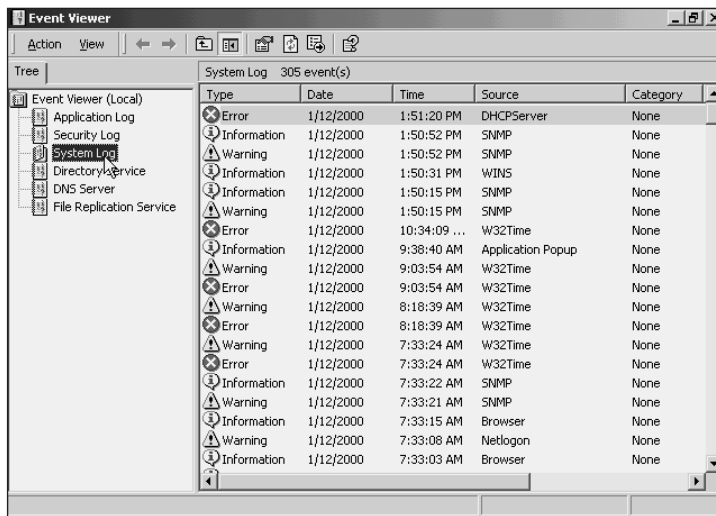


Figure 16-1 Event Viewer

The **system log** records information about system-related events such as hardware errors, driver problems, and hard drive errors. The **security log** records access and security information about logon accesses and file, folder, and system policy changes. If you have auditing set up, for instance file auditing, use the security log to track each audited event, such as a successful or failed attempt to access a file. If you choose to audit an account or folder, the audit data is recorded in the security log. The **application log** records information about how software applications are performing, if the programmer has designed the software to write information into the log. For example, if a software error occurs, it may be recorded in the log. The **Directory Service log** records events that are associated with the Active Directory, such as updates to the Active Directory, events related to the Active Directory's database, replication events, and startup and shutdown events. The **DNS Server log** provides information about

instances in which (1) DNS information is updated, (2) there are problems with the DNS service, and (3) the DNS Server has started successfully after booting. File replication activities are recorded through the **File Replication Service log**, which contains information about (1) changes to file replication, (2) when the service has started, and (3) completed replication tasks.

Log events are displayed with an icon that indicates the seriousness of the event. An informational message, such as notification that a service has been started, is prefaced by a blue “i” displayed in a white comment circle; a warning, such as that a CD-ROM is not loaded, is depicted by a black “!” (exclamation point) that appears on a yellow caution symbol; and an error, such as a defective disk adapter, is indicated with a white “x” that appears inside a red circle (see Figure 16-1). Each log displays descriptive information about individual events, such as the following information provided in the system log:

- Type of event—information, warning, or error
- Date and time of the event
- Source of the event, which is the software application or hardware reporting it
- Category of event, if one applies, such as a system event or logon event
- Event number, so the event can be tracked if entered into a database (associated events may have the same number)
- User account involved in the event, if applicable
- Name of the computer on which the event took place

The Event Viewer is opened by clicking Start, pointing to Programs, pointing to Administrative Tools, and clicking Event Viewer. Two other ways to access the Event Viewer are as an MMC snap-in or from the Computer Management tool, under System Tools in the tree. The Event Viewer contains options to view all events or to set a filter so only certain events are viewed, such as only error events.

The first time you start the Event Viewer, it shows the system log by default, as in Figure 16-1. To view one of the other logs, click that log in the tree under Event Viewer. To view the detailed information about an event, double-click the event. Read the description of the event for more information. In Figure 16-2, the Event Properties dialog box shows that the DHCP/BINL service is not authorized on the network. This error means that the DHCP server is not authorized in the Active Directory, and this problem should be corrected as soon as possible, because DHCP cannot lease IP addresses to clients.

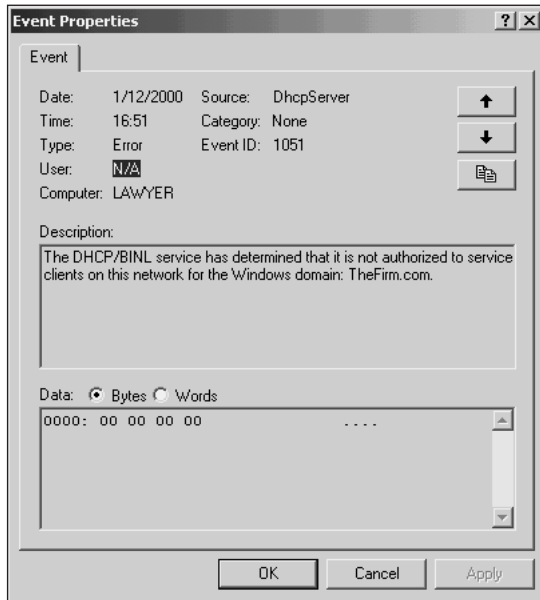


Figure 16-2 Viewing a system log event



The event logs are a good source of information to help you troubleshoot a software or hardware problem. For example, if Windows 2000 Server crashes unexpectedly, reboot and look at the logs as a first step. A memory allocation or disk problem may be found quickly through the help of the system log. If a software application hangs, check the application log for information.

All of the event logs in the Event Viewer have a filter option to help you quickly locate a problem. For example, you can design a filter to show only events associated with the disk drives or only events that occurred on the previous afternoon (try Hands-on Project 16-1 to use the Event Viewer and create a filter). The events can be filtered on the basis of the following criteria:

- Event type, such as information, warning, error, success audit (for the security log), failure audit (for the security log)
- Source of the event, such as a particular service, software component, or hardware component
- Category of the event, such as a security change
- Event ID, which is a number assigned by the Event Viewer to identify the event
- User associated with the event
- Computer associated with the event
- Date range
- Time of day range

For instance, to build a system log filter to view only the error events for the Server service, you would use the following steps:

1. Start the Event Viewer and display the system log.
2. Right-click System Log in the tree, and click Properties.
3. Click the Filter tab.
4. Select Server in the Event source box (see Figure 16-3).
5. Remove the check marks from all event types except for Error.
6. Click OK.

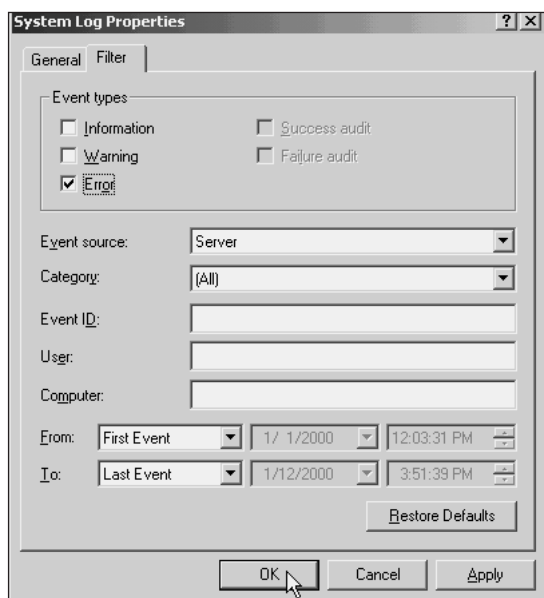


Figure 16-3 Creating a system log filter

The event logs quickly fill with information, and you should establish from the beginning how you want the logs maintained. There are several ways to maintain the logs, as follows:

- Size each log to prevent it from filling too quickly.
- Regularly clear each log before it is full.
- Automatically override the oldest events when a log is full.

Some network administrators prefer to save the log contents on a regular basis, such as weekly or monthly. Others prefer to allow the logs to overwrite the oldest events. It is recommended that you develop a maintenance schedule to save the log contents for a designated time period, because the logs contain valuable information about historical server activity. For example, if a financial auditor needs to see information about who is accessing the payroll folder, you can set up auditing on that folder and then save the security log data that contains the audited events.

To tune the event logs, open the Event Viewer and select each log you want to tune, one at a time, and click Properties. In the *Log size* box on the General tab, set the log size in the Maximum log size ____ KB box. Set the maximum log size to match the way you want to handle the logs. The default size is 512 KB. For example, if you want to accumulate two weeks of information, set the size to enable that much information to be recorded, for instance 2048 KB. You will need to test this setting for a few weeks to make sure that the size you set is adequate. A common way to make sure that an event log is never completely filled is to use one of these options: *Overwrite events as needed* or *Overwrite events older than ____ days*. For example, you might set up the log to overwrite events that are older than 14 days, so that you continuously have at least two weeks of information stored in a log (see Figure 16-4).

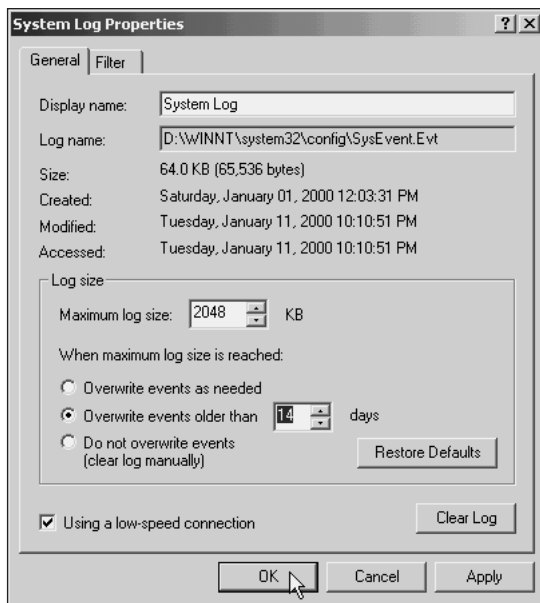


Figure 16-4 Configuring event log settings

There also are options to save and clear the individual logs. To save a log, right-click the log in the tree, click *Save Log File As*, enter a name for the log file, and click *Save*. You can save the log as one of three kinds of files:

- *.evt*, which is saved in event log format
- *.txt*, which is saved as a tab-delimited text file that can be imported into a spreadsheet
- *.csv*, which is saved as a comma-delimited text file that can be imported into a spreadsheet

When you are logged on as Administrator, the event log files are saved by default in the folder `\Documents and Settings\Administrator\My Documents`. To clear a log, right-click the log in the tree and click *Clear all Events*.

TROUBLESHOOTING CONFIGURATION PROBLEMS

In earlier chapters, you learned many troubleshooting techniques for configuring specific Windows components and other Windows 2000 Server software. In addition to those techniques, there are some general steps you can take to troubleshoot configuration problems:

1. The event logs are a good place to start when you are looking for a configuration error. Often this kind of error is recorded in a log, because a service cannot start or the software is unable to function. After you install a Windows component or other software, check the appropriate event logs to make sure no configuration errors are reported. For example, after you install DNS, check the system and DNS Server logs for errors and warnings. Do the same after you install DHCP, checking the system log as illustrated earlier (refer to Figure 16-2).
2. After you install a Windows component, check the Control Panel Add/Remove Programs tool and then click Add/Remove Windows Components to make sure that there are no additional configuration tasks that you have missed. Figure 16-5 shows the display when RIS has been installed, but is not yet configured.

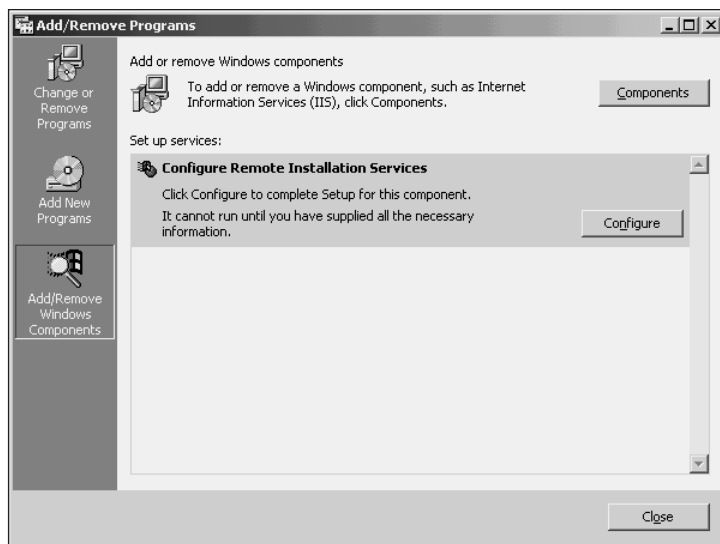


Figure 16-5 Checking to make sure a Windows component is configured

3. If you are unsure about the configuration steps for some elements of Windows 2000 Server, use the Configure Your Server tool in the Administrative Tools menu. This tool will help you install and configure software such as the Active Directory, file sharing, printer sharing, Web and media servers, DHCP, DNS, RAS, routing, component services, terminal services, database servers, e-mail servers, message services, support tools, and optional components.

4. The Control Panel is another place in which you can troubleshoot configuration problems. For example, you can configure the display and update new display drivers, using the Display icon. The Printers icon can be used to find and correct a printer setup problem.
5. Use the Network and Dial-up Connections tool to check the network connectivity configuration, for example to troubleshoot a configuration problem with TCP/IP or with a NIC.
6. The Computer Management tool is a central place from which to troubleshoot many kinds of configuration problems. Access it from the Administrative Tools menu (or right-click My Computer and click Manage). Use the System Information selection in the tree to troubleshoot system, hardware, Windows components, software, and Internet Explorer configuration problems. For example, you can quickly troubleshoot a hardware resource conflict by opening the Computer Management tool, double-clicking System Information in the tree, double-clicking Hardware Resources, and clicking Conflicts/Sharing (try Hands-on Project 16-2). Another powerful option that is included in the Computer Management tool is the Device Manager (try Hands-on Project 16-3). For example, to verify that a floppy disk controller has no resource conflicts, open Device Manager under System Tools and then double-click Floppy disk controllers in the right pane, double-click the controller, such as Standard floppy disk controller, click the Resources tab, and look for conflicts in the Conflicting device list (see Figure 16-6). Also, as you have learned in several earlier chapters, configuration problems with a service, such as a service that does not start automatically, can be solved by opening Services and Applications in the Computer Management tool.

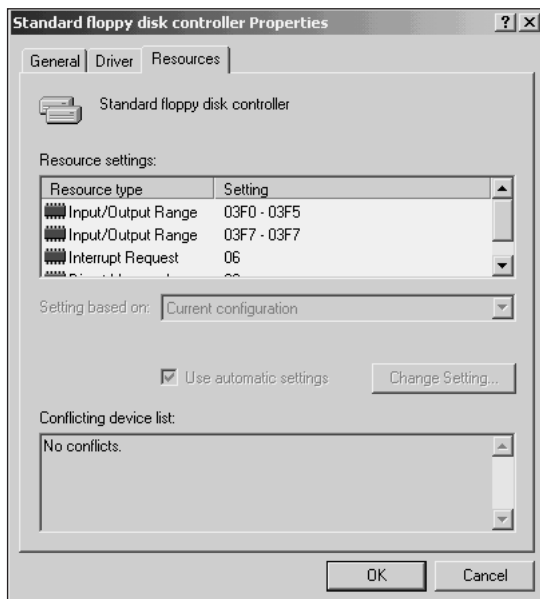


Figure 16-6 Using Device Manager to find a configuration conflict

Troubleshooting Client, Server, and Network Connectivity Problems

A server or workstation may have problems connecting to the network or to other computers on the network for several reasons. When you experience a connection problem, try the following:

- Check to see if only one station, several stations, or all stations are having problems.
- Check that the server's NIC driver is properly installed and is a current version.
- Use the NIC test software to determine that the NIC is functioning, and reseal or replace the NIC if it fails the test.
- Verify the protocol setup through the Windows 2000 Network and Dial-up Connections tool, or, for Windows 95, 98, and NT, use the Network icon. One of the most common problems on networks that do not use DHCP is that the IP address or subnet mask is inappropriately configured.
- Make sure that the NIC properties are configured correctly. For example, a NIC configured for full-duplex will not communicate properly on a network in which hubs and switches are configured for half-duplex. Also, make sure that the media type (cable setting) is configured to match the type of cable connected to the NIC. A NIC configured for 10Base2 or 100BaseTx will not function on a 10BaseTx network.
- Check to ensure that the correct protocols are installed for network communications. Also, make sure that if NWLink is installed, the packet type is configured to match the packet type used in IPX/SPX communications; for example use a packet type for Ethernet 802.2, Ethernet 802.3, Ethernet II, or Ethernet SNAP.
- Make sure that all server clients are configured to use the correct domain or workgroup to access the server. Also, make sure that server clients are identified by a unique computer name.
- Check the cable connection into the NIC, or reconnect the cable.
- Examine the network cable to the NIC for damage.

For example, if you are using an out-of-date NIC driver, the server or workstation may have difficulty connecting to the network, or it may periodically lose connection. Another problem on Ethernet networks is that computers may be using different versions of Ethernet. On a Microsoft-based network that uses NWLink, check the protocol setup to make sure that all computers are using the correct frame type. To check NWLink, click Start, point to Settings, click Network and Dial-Up Connections, right-click Local Area Connection, click Properties, and double-click NWLink IPX/SPX/NetBIOS Compatible Transport Protocol. Check the frame type and network number to make sure they are the same as those used by the NetWare servers (see Chapter 6).

If a computer is unable to communicate because TCP/IP addressing is not configured correctly, fix the problem by opening the Network and Dial-up Connections tool, right-clicking

Local Area Connection, clicking Properties, and double-clicking Internet Protocol (TCP/IP). Make sure that the IP address and the subnet mask are configured correctly, if DHCP is not in use on the network. Remember that it is important for each computer to have a unique IP address that is consistent with other IP addresses used on the network. If DHCP is in use, make sure that *Obtain an IP address automatically* is selected.

Another connectivity problem to check is the cable medium setting in the software. A NIC set for coaxial cable will not communicate if it is connected to twisted-pair cable. In Windows 2000 Server you can check this by starting the Network and Dial-up Connections tool, right-clicking Local Area Connection, clicking Properties, clicking the Configure button, clicking the Advanced tab, and clicking Media Type (see Figure 16-7).

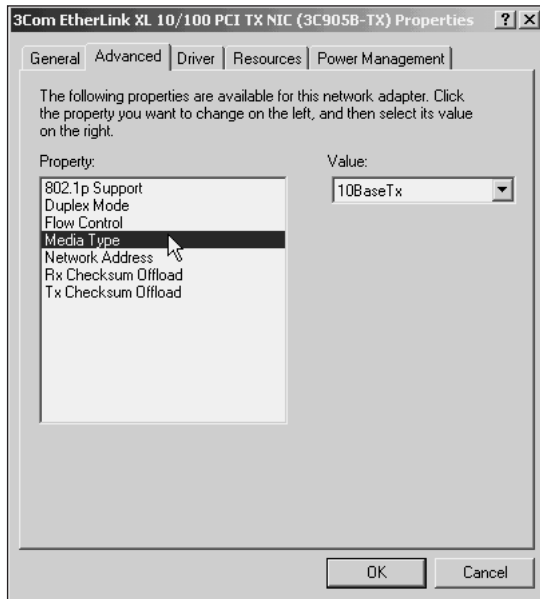


Figure 16-7 Troubleshooting the NIC media type

When multiple users have trouble accessing a server, check to make sure that the server is on, that it is completely booted, and that it has a good network connection in terms of the NIC (try Hands-on Project 16-3), connector, and cable. Always make sure that servers have the latest NIC drivers. Sometimes users cannot connect to a server because one or more disk drives have failed, or a SCSI adapter is malfunctioning. Also, check the network equipment that the user's transmission must pass through to reach the server. Table 16-1 presents a variety of connectivity problems and their solutions.

Table 16-1 Troubleshooting Connectivity Problems

Connectivity Problem	Solutions
The NIC will not connect to the network (no computers are visible in My Network Places).	<ol style="list-style-type: none"> 1. Check the system log for reported problems. 2. Check the cable and cable connection to the NIC for damage or for a loose connection. Do the same for the connection into the wall or hub/switch. Also, check to make sure intermediate network equipment (such as hubs, switches, and routers) is working. 3. Check that the media type (cable type) set for the NIC is the same as is used on the network. 4. Check to make sure that the NIC driver is installed, that it is the most current, and that bindings are set. 5. Check to make sure that the correct protocol is installed and that all protocol parameters are correct, including packet type for NWLink. 6. Run the NIC manufacturer's NIC diagnostics program to locate problems. 7. Replace the NIC with one you know is working.
Windows 2000 Server periodically disconnects from the network, or it experiences a connectivity problem when a particular computer is logged on.	<ol style="list-style-type: none"> 1. Check the cable segment to make sure it is within IEEE specs for distance and cable type. Also, check for electrical interference on the cable segment, check the cable and connector for damage, check for a problem with that port on the network hub/switch, and check for a problem with the server's or the workstation's NIC. 2. Make sure no other station on the network has the same computer name. 3. If using TCP/IP, make sure no other station is using the same IP address.
Windows 2000 Server has difficulty maintaining a reliable connection as a client or when acting as a gateway to a NetWare server via NWLink.	Try resetting the MaxPktSize for IPX communications. To do this, edit the Registry path <code>\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Nwlnk\Parameters\Adapters\(<i>adapter device address</i>)</code> and change the MaxPktSize value from 0 to a decimal 1000 (in either Regedit or Regedt32, double-click the parameter, and enter 1000 in decimal).
Computers on a Microsoft network experience Network Neighborhood and My Network Places display problems when Windows 3.11 clients are logged on.	Windows 3.11 clients may contend with a Windows 2000 or NT server or workstation to act as the master browser. On every Windows 3.11 client, edit the System.ini file to have the line: <code>MaintainServerList=no</code> .
Clients cannot run logon scripts when connecting to a Windows 2000 server.	Check to make sure the location of logon scripts matches the location specified via the Local Users and Groups or Active Directory Users and Computers tool for each account.

Table 16-1 Troubleshooting Connectivity Problems (continued)

Connectivity Problem	Solutions
Clients cannot access a shared directory or printer.	Check the rights, group memberships, share permissions, and regular permissions associated with the shared resource.
Clients cannot log on to the Windows 2000 server.	Make sure that the Windows 2000 computer is powered on and properly connected to the network, and that the Server, Workstation, and Computer Browser services are started (use the Services tool in the Administrative Tools menu).
Windows 2000 is not responding as an SNMP agent.	<ol style="list-style-type: none"> 1. Make sure that the SNMP service is installed and is set to automatically start when the computer is booted. 2. Make sure that the SNMP and SNMP Trap services are started (use the Services tool in the Administrative Tools menu). 3. Make sure that the community names are set correctly.
Windows 2000 generates excessive Routing Information Protocol (RIP) packets via NWLink, causing excessive network traffic.	Windows 2000 Server can be set up as an IPX router on a network that also has Novell NetWare servers. Normally, it is better to allow the NetWare servers and network routers to handle IPX routing and to leave this function turned off in Windows 2000. To turn it off, click Start, point to Programs, point to Administrative Tools, click Routing and Remote Access, double-click IPX Routing under the tree, click RIP for IPX, double-click Local Area Connection (in the right pane), and remove the check from <i>Enable RIP on this interface</i> . (If SAP is not used by the NetWare servers, also disable SAP by double-clicking SAP for IPX in the tree, double-clicking Local Area Connection, and removing the check from <i>Enable SAP on this interface</i> .)
TCP/IP packets sent from Windows 2000 are not routed.	Enable the IP routing manager by clicking Start, pointing to Programs, pointing to Administrative Tools, clicking Routing and Remote Access, double-clicking IPRouting under the tree, clicking General, double-clicking Local Area Connection (in the right pane), and making sure that <i>Enable IP router manager</i> is checked.

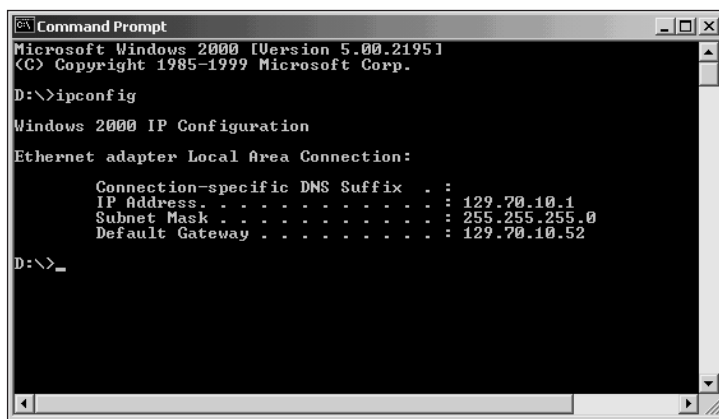
NIC Broadcast Problems

Sometimes a NIC malfunctions and broadcasts continuously, creating a broadcast storm that causes the entire network to slow down. A broadcast storm is a condition in which so many broadcasts are sent at the same time that the network bandwidth is saturated and the network slows significantly or times out. Use Network Monitor or System Monitor, as you learned in Chapter 15, to trace a malfunctioning NIC.

Troubleshooting TCP/IP Connectivity

One area that network administrators often troubleshoot is TCP/IP connectivity. For example, a common problem is the use of duplicate IP addresses. This can happen in situations where static IP addressing is used, with the network administrator or user typing in the IP address and subnet mask when the computer is set up. If two computers are using the same IP address, one or both will not be able to connect to the network, if both attempt to connect at the same time; or both are likely to experience unreliable communications such as sudden disconnections.

Some TCP/IP utilities, such as Telnet, have IP troubleshooting tools built in. The same is true for workstations and servers running TCP/IP-compatible operating systems, such as Windows 2000 and Windows 98. You can test the IP address of a Windows 98 or Windows 95 computer by opening the MS-DOS Prompt window from the Start button, Programs option. Type *winipcfg* to view a dialog box showing the adapter address (MAC or Ethernet), IP address, subnet mask, and other information for that workstation. You can run a similar test in Windows 2000 Server and Professional (also Windows NT) from the Command Prompt window by clicking Start, pointing to Programs, pointing to Accessories, clicking Command Prompt, typing *ipconfig*, and pressing Enter (see Figure 16-8). If the server is using an IP address that is identical to the address used by another networked computer that is turned on, the subnet mask value is 0.0.0.0 when you run one of these utilities.



```

Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

D:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

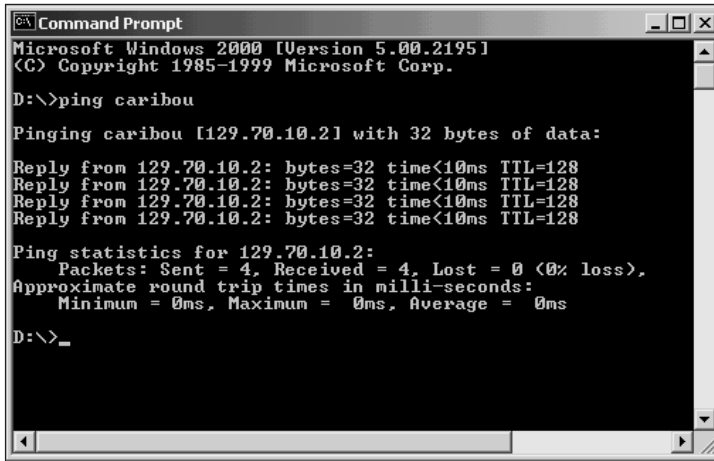
    Connection-specific DNS Suffix . . : 
    IP Address. . . . . : 129.70.10.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 129.70.10.52

D:\>_

```

Figure 16-8 Using *ipconfig*

Another tool for testing TCP/IP connections is the *ping* utility. You can poll the presence of another TCP/IP computer from the Windows 95 or Windows 98 MS-DOS Prompt or Windows NT or 2000 Command Prompt window by typing *ping* and the address or computer name of the other computer. Many server administrators use *ping* to quickly test the presence of a server or mainframe from their office when there are reports of connection problems to that computer. *Pinging* a server on a network in another state or remote location also enables you to quickly test if your Internet connectivity is accessible from your office workstation. Figure 16-9 illustrates the *ping* utility as used from Windows 2000.



```
Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

D:\>ping caribou

Pinging caribou [129.70.10.2] with 32 bytes of data:

Reply from 129.70.10.2: bytes=32 time<10ms TTL=128
Reply from 129.70.10.2: bytes=32 time<10ms TTL=128
Reply from 129.70.10.2: bytes=32 time<10ms TTL=128
Reply from 129.70.10.2: bytes=32 time<10ms TTL=128

Ping statistics for 129.70.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\>_
```

Figure 16-9 Using *ping*

Netstat is a utility for Windows 2000, NT, 98, and 95 that is a quick way to verify that a workstation or server has established a successful TCP/IP connection. This utility provides information about TCP and UDP connectivity. Sometimes a TCP/IP session to a server or mainframe computer hangs. You can determine this by entering *netstat -e* from the MS-DOS Prompt or Command Prompt window at that computer. Two columns of received and sent data are displayed. If these columns contain 0 bytes, it is likely the session is hung. If it is, and the computer is running Windows 2000, use the Network and Dial-up Connections tool to disable the connection and then to reconnect. You can do this by opening the Network and Dial-up Connections tool, double-clicking Local Area Connection, and clicking Disable. To reestablish the connection, open the Network and Dial-up Connections tool and double-click Local Area Connection. For computers running Windows NT, 98, and 95, reboot the computer and try again. Disabling the connection or rebooting will reset the NIC and the TCP/IP connectivity to make sure you have a clean connection. The *netstat -e* command also provides a quick indication of the number of transmission errors and discarded packets detected at that computer's NIC. For a more comprehensive listing of communication statistics, type *netstat -s*. Table 16-2 lists some useful diagnostics available from the MS-DOS and Command Prompt windows in Windows 2000, Windows NT, Windows 98, and Windows 95. Try Hands-on Project 16-4 to practice some of these commands.

Table 16-2 Windows 2000, NT, 98, and 95 Diagnostic Commands for TCP/IP Connectivity

Diagnostic Command	Function
<i>winipcfg</i> (Windows 98/95) <i>ipconfig</i> (Windows 2000/NT)	Displays information about the TCP/IP setup at that computer (enter <i>ipconfig /?</i> or <i>winipcfg /?</i> to view all of the options for these commands)
<i>ping</i>	Polls another TCP/IP node to verify that you can communicate with it (enter only <i>ping</i> to view all of the options for this command)
<i>netstat</i> (-a, -e, -s)	Displays information about the TCP/IP session from that computer (enter <i>netstat /?</i> to view all of the options for this command)
<i>nbtstat</i> (-n)	Shows the server and domain names registered to the network (enter only <i>nbtstat</i> to view all of the options for this command)
<i>tracert</i> (server or host name)	Shows the number of hops and other routing information on the path to the specified server or host (enter only <i>tracert</i> to view all of the options for this command)

Troubleshooting Cable Problems

Network cabling is one of the most common sources of network problems. Cabling problems have many symptoms, such as disconnecting workstations, slow network services, a high level of packet errors, and unreliable data transmission. If you have reports of any of those problems, one place to start is by investigating the network cabling. There are several things to check related to cabling problems, such as cable length, cable type, cable impedance, terminators, connectors, and open or short circuits.

Network problems may show up on the Network Monitor as dropped frames, CRC errors, or other error conditions. A **cyclic redundancy check (CRC)** is an error-checking technique used in network protocols to signal a communications problem. **Dropped frames** are those that are discarded because they are improperly formed, for example failing to meet the appropriate packet size.

On a small network, it is good practice for the server or network administrator to periodically inspect the visible cabling for damage. Cable may be pinned under a table leg, excessively bent or knotted, or damaged from exposure to a portable heater. Also, cable connectors may be broken or have an exposed wire. The best solution for damaged cable is to replace it immediately. On large networks, cable problems can be traced through the use of network test equipment or by means of enterprise-wide network-monitoring software.

The most economical solution for a small network is to use Network Monitor and System Monitor along with inexpensive test equipment such as a cable scanner, which tests the length of cable and looks for electrical problems. For a small to medium-sized network, if a network problem cannot be found immediately, it may be most cost-effective to hire a network professional rather than to purchase equipment and spend many personnel hours locating a problem. The network professional will likely have equipment to help quickly locate and solve a problem, including problems with fiber-optic cable. Table 16-3 lists common cable problems that you should look for and ways to troubleshoot them.

Table 16-3 Troubleshooting Cable Problems

Cable Problem	Solutions
A cable segment that is too long	If a network segment is extended beyond the IEEE specifications, there will be communications problems affecting all nodes on that segment. Use a cable scanner, which is a device that tests network cable, to measure the distance of the cable.
Mismatched or improper cabling	Check the labeling on the cable jacket to make sure it is right for your network.
Defective or missing terminator on coaxial cable	A segment with a defective or missing terminator responds like one that is too long, and usually does not work. Workstations on the segment may disconnect, experience slow network response, or receive network error messages. If your cable scanner shows that the segment distance is invalid, check the terminators.
Improper grounding	Proper grounding is critical to packet transmission on the cable. Without it, the network packet transmissions will have many CRC errors. Ethernet frames include this check to ensure the reliability of data transfer from the source node to the recipient node. The Network Monitor reports CRC errors in the Total pane.
Open or short circuits	Use a cable scanner to find opens and shorts. Also, check the Network Monitor Total pane error statistics for CRC errors and dropped frames.
Electrical and magnetic interference	Electrical and magnetic interference results in excessive noise or jabber on the cable. This happens when the cable is run too close to an electrical field, for example over fluorescent lights in the ceiling or through a machine shop with heavy electrical equipment. Check the cable for these possibilities.
Defective connector	A faulty connector can cause a short or open on the cable. If several workstations on a segment are experiencing problems, or a segment is automatically shut down by network equipment, this may be due to a cable connector on a workstation or server. Use a cable scanner to identify shorts and opens due to a faulty connector. Also, the Network Monitor can help through identifying a high rate of CRC errors and dropped frames.
Improper coax connectivity at the wall outlet	A T-connector should not be placed directly on a wall outlet because the topology for a coax segment must be a bus or "in series."
Improper distance between connections	Two adjacent stations may have network communications problems, if the distance between their connectors is too short. The same is true if the distance is too short between a node and a hub. For example, on a thinnet coaxial Ethernet segment, the minimum distance between nodes is 0.5 meters. For twisted-pair cable, the minimum distance between two nodes, between a node and a hub, or between the wall outlet and a node is 3 meters. Check to be certain that all workstations are separated according to IEEE specifications.

TROUBLESHOOTING NETWORK PRINTING PROBLEMS

Printing problems are common on a network. The best advice is to check out the simplest solutions first. These include the following:

- Make sure the printer has power.
- If the printer is physically connected to a workstation or server, check to make sure that the computer is turned on and working.
- Be certain the printer is online (that is, the online light or button is active).
- Press the printer reset button, in case the printer has not fully reset after the last print job.
- Make certain all printer trays have paper.
- Check that the printer data cable is properly connected between the computer and the printer.
- Check that the network cable is properly connected when a print server card is used in the printer.
- Stop and restart the Windows 2000 Server Print Spooler service.

These are obvious solutions, but they are not always checked first. Perhaps the most overlooked solution is to press the reset button on the printer (if it has one). When several people share one printer, it may be printing documents with different fonts and formats. A slight miscue at the printer or in a printer connection may cause it to miss the software reset instruction sent at the beginning of each document.

If the problem is related to the server or workstation, the areas most likely to be responsible are the following:

- The printer driver is improperly installed and selected for the print job.
- The printer share is not enabled.
- The printer share permissions are set incorrectly.
- The software used to produce the print job is incorrectly installed at the workstation.
- The wrong print job data type is set up.
- The wrong print monitor is installed.
- The wrong protocol is installed (for example, Microsoft DLC may need to be installed at the print server and at workstations for some types of older Hewlett-Packard printers).

Table 16-4 provides a series of practical steps you can take to resolve different types of network printing problems.

Table 16-4 Troubleshooting Network Printing Problems

Network Printing Problem	Solutions
Only one character prints per page.	<ol style="list-style-type: none"> 1. If only one workstation experiences this problem, reinstall the printer driver on that workstation, using the Add Printer Wizard. 2. If all workstations are experiencing the problem, reinstall the printer and printer driver at the computer or print server offering the printer share (using the Add Printer Wizard). 3. Check the print monitor and data type setup.
Some users get a no-access message when trying to access the printer share.	Check the share permissions. Make certain the clients belong to a group for which at least Print permission has been granted and that none of the groups to which these users belong is denied Print permissions.
Printer control codes are on the printout.	<ol style="list-style-type: none"> 1. If only one workstation experiences the problem, reinstall the printer driver on that workstation, using the Add Printer Wizard. Also, make sure the software generating the printout is installed correctly. 2. If all workstations are experiencing the problem, reinstall the printer and printer driver at the computer or print server offering the printer share (using the Add Printer Wizard). 3. Make sure the share is set up for all operating systems that access it, that the right print monitor is installed, and that the right data type is used.
A print server card is used on the printer and shows an amber or red data error light.	Power off the printer. Disconnect the network cable to the printer. Reconnect the network cable and turn on the printer.
A print job shows that it is printing, the printer looks fine, but nothing is printing.	<ol style="list-style-type: none"> 1. Open the Printers folder and click the icon for the printer. Check for a problem with the print job at the top of the queue. If it shows that the job is printing, but nothing is happening, delete the print job because it may be hung. Resubmit the print job. 2. Also, try stopping and restarting the Print Spooler service (warn users first).
The wrong print form is used.	Check the setup of the document in the software at the client.
A workstation cannot view the printer share in Network Neighborhood or in My Network Places.	<ol style="list-style-type: none"> 1. Check the network connection to that workstation, including connectors, cable, network hub, and the workstation's NIC. 2. Also, check the protocol setup at the workstation. Make sure that the workstation is a member of the domain, if the Active Directory is implemented.

Table 16-4 Troubleshooting Network Printing Problems (continued)

Network Printing Problem	Solutions
Some clients find that the ending pages are not printed for large print jobs.	Check the disk space on the server or workstation in which the job is spooled. It may not have enough space to fully spool all jobs.
On some long print jobs, pages from other print jobs are found in the printout.	Set the printer properties for the printer so it starts printing only after all pages are spooled. To do that, open the Control Panel, open the Printers folder, right-click the icon for the printer, click Properties on the shortcut menu, click the Advanced tab, click the radio button for <i>Spool print documents so program finishes printing faster</i> , click the radio button for <i>Start printing after last page is spooled</i> , and click OK.
Extra separator pages are printed, or print jobs seem to get stuck in the printer for all users.	Check the print processor in use. To do that, open the Control Panel, open the Printers folder, right-click the icon for that printer, click Properties, click the Advanced tab, click the Print Processor button, and check the print processor in use. Also check the data type. If the problem continues, try a different data type.
Some clients occasionally send a document that prints garbage on hundreds of pages before anyone notices and can stop the printing.	Have the spooler automatically hold print jobs that contain the wrong printer setup information. To do that, open the Printers folder, right-click the icon for that printer, click Properties, click the Advanced tab, click the check box to <i>Hold mismatched documents</i> , click OK on the Properties dialog box.

TROUBLESHOOTING SECURITY AND ACCESS PROBLEMS

One of the most common network problems is that users are not able to log on or access desired resources. Users can forget their passwords or change their passwords but not remember the new ones they created, or they may be assigned inappropriate permissions. As a security precaution, Windows 2000 Server does not allow the administrator to look up a user password, because the password is hidden by asterisks. As administrator, you do have the ability to change a user's password through the Local Users and Groups and Active Directory Users and Computers tools (depending on whether the Active Directory is installed). If a user cannot remember a password, you can set a new password with the provision that the user must change the password at next logon, allowing him or her to enter (and hopefully remember!) a new password. To change a password using the Active Directory Users and Computers tool, for example:

1. Click Start, point to Programs, point to Administrative Tools, and click Active Directory Users and Computers.
2. In the tree, open the appropriate container, such as Users, that houses the user account.

3. Find the account in the right-hand pane, right-click the account, and click Reset Password.
4. Enter the new password, confirm it, and click the box *User must change password at next logon*.
5. Click OK.

Many organizations have policies about how to communicate a new or changed password to a user, because of recommendations made by their financial auditors. In those organizations, the server administrator may hand-deliver the password to the user instead of communicating it over the telephone or through e-mail, to ensure that the password directly reaches the account owner. Another method is to send the password in a sealed envelope through the company mail. Also, some auditing recommendations have the server administrator keep a record of each newly created account and all password changes made by the server administrator for that account.

Sometimes a user or a group of users is unable to access a resource, such as a shared folder, subfolder, or a shared printer, because there is a problem with the permissions. One way to diagnose the problem is to temporarily audit the resource to show failed access, and then have the user try accessing the resource. Next check the security log, because it creates an event that reports on the access problem. Another way to diagnose an access problem is to examine each group to which a user belongs and make sure that access to a particular resource is not denied in one of those groups.

Some administrators have one or more test accounts that enable them to replicate an access problem, particularly when the problem involves a group membership. This also is a good way to test the security available to a group of users before releasing the resources to those users, for example when you implement a new application or database. Another way to test the problem is to log on to the Administrator account and determine if that account can access the resource. While you are logged on as Administrator, check the share permissions and the folder and file permissions assigned to each group that accesses the resource, and change the permissions, if necessary, to grant access to a user or a group. Keep in mind, for example, that there may be a mismatch between the different types of permissions so that the user or group has access at the share level, but not at the folder or file level. Also, check for conflicts created because a user belongs to one group that has the right permissions and to another group that is denied access. (Permissions are covered in detail in Chapter 9.)

If the Administrator account cannot access the resource, the next step is to take ownership of the resource and then grant permissions to the appropriate groups and users. For example, ownership of a folder is taken by opening the Properties dialog box for that folder, clicking the Security tab, clicking the Advanced button, and then clicking the Owner tab. (Try Hands-on Project 16-5 to practice taking ownership.)

Tracking Intruders

Sometimes you may suspect that there is a problem caused by an intruder trying to gain access to a resource for which the intruder is not authorized. You can monitor this situation

by auditing the resource and by using System Monitor. Set up auditing to audit the resource for failed access, and then check the security event log to look for instances of the failed access. To more broadly watch for intruders and track access-denied situations, open System Monitor and monitor the Server object and the Errors Access Permissions and the Errors Granted Access counters. Also, you can use System Monitor to watch for intruders who are attempting to log on to the server. To do this, monitor the Server object and the Errors Logon counter.

Troubleshooting Security Using the System Security and Analysis Tool

Even though you have been careful about setting up security and group policies, there may still be omissions in the security you have established. Also, as time passes, the security requirements on a server or in a domain may change. Windows 2000 Server offers the System Security and Analysis tool, which is an MMC snap-in to help you monitor and analyze security. This tool works by creating a database from which to configure a server and perform a security check. For example, if you are setting up the first DC, you can use this tool to configure the server for the default domain security policy. Later, you can use the tool to perform an analysis of the policy, to determine if you need to make modifications on the basis of growth in server use. You can use the tool to import an existing template or to import a new security template that you have created (see Chapter 4). The database may be built from an existing group policy or a security template, or you can construct a database the first time that you run the tool. After a database is in place, for example for the domain or for an OU, you should periodically analyze it to see if it meets the system's security recommendations.

To run the System Security and Analysis tool to analyze an existing database (group policy):

1. Click Start, click Run, and type mmc. Click OK.
2. Maximize the console windows, if necessary.
3. Click the Console menu and click Add/Remove Snap-in.
4. Click the Add button, and then double-click Security Configuration and Analysis.
5. Click Close and then OK.
6. Right-click Security Configuration and Analysis in the tree, and click Open Database.
7. Click the database that you want to analyze, and click Open.
8. Right-click Security Configuration and Analysis again, and then click Analyze Computer Now.
9. Make sure that the error log file location is appropriate for the error log that the tool will create, and then click OK. The tool displays an Analyzing System Security dialog box to show what it is checking (see Figure 16-10).

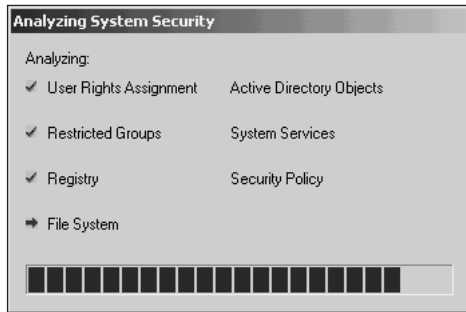


Figure 16-10 Checking system security

10. If the results are not displayed automatically, to view the results of the analysis that are recorded in the log file, right-click Security Configuration and Analysis, and then click View Log File.
11. Scroll through the log file in the right pane (see Figure 16-11).

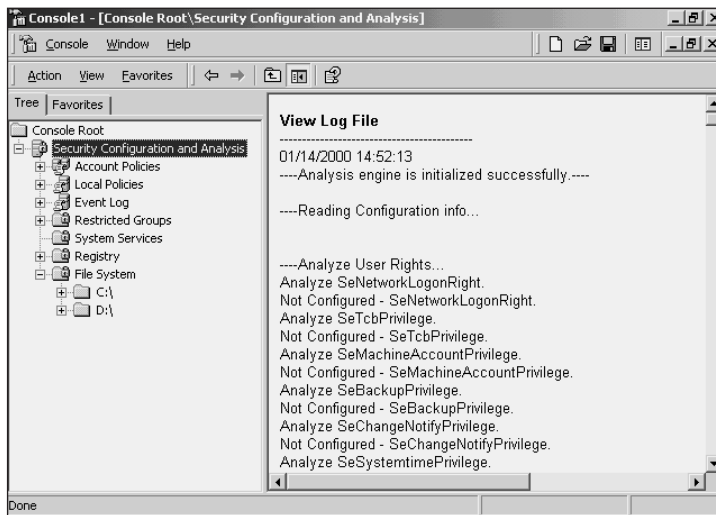


Figure 16-11 Security analysis results

Examine the log file for any areas in which you want to improve security. Also, you can examine existing security settings by selecting any object in the tree. For example, in the database shown in Figure 16-11, you might double-click Account Policies and then click Password Policies in the tree to view the password policy settings, such as the settings for *Enforce password history* and *Maximum password age*. Try Hands-on Project 16-6 to practice analyzing security.

RESOLVING BOOT PROBLEMS

Sometimes the server encounters a hardware problem and cannot be booted, displays a blue error screen during the boot process, or hangs. There are several possible causes of boot failures, such as the following:

- Disk failure on the drive or drives containing the system and boot files
- A corrupted partition table
- A corrupted boot file
- A corrupted master boot record
- A disk read error

In most cases the first step is to power off the computer and try rebooting. Often this will work in instances where there is a temporary disk read error during the first boot attempt, which is corrected on the second try. Also, one or more data storage registers may be out of synchronization in the CPU, causing a transient problem. Rebooting resets the CPU registers. If there are multiple drives in the computer, a disk controller may need to be reset, which is accomplished by rebooting.



The best way to reboot for clearing a temporary error is to turn the power off, wait several seconds for the hard disk drives to fully come to a stop, and then turn on the power. This causes all components to completely reset. If, instead, you reboot using a reset button, some components may not fully reset.

Troubleshooting by Using Safe Mode

If a simple reboot does not fix the problem, or if you have installed new software or drivers, or changed the server configuration, and the server does not properly boot, try using the advanced options for booting—accessed by pressing F8 as soon as the computer boots—which include starting the computer in safe mode. **Safe mode** boots the server using the most generic default settings (for example for the display, disk drives, and pointing device) and only those services needed to boot a basic configuration. After you boot into safe mode, you have the opportunity to further troubleshoot the problem.

For example, if you installed software or a driver that caused a problem with the boot process, then you can boot into safe mode and remove that software or driver. Or, perhaps you have replaced the mouse with a trackball and installed the new driver for the trackball, but after you reboot, there is no pointer on the screen when you move the new trackball. You can boot into safe mode, reinstall the old driver and mouse, and contact the trackball vendor for a solution or new driver. Or, if you changed the server's configuration, for example by setting up an additional page file or installing a Windows component, and the server does not properly boot, you can restore the original page file settings or remove the Windows component, while in safe mode.



If you contact a Microsoft technician for help with a server problem, often she or he will ask you to boot in safe mode in order to execute troubleshooting steps.

Table 16-5 lists the advanced booting options that are available when you press F8 at the beginning of the boot process, and Figure 16-12 shows the Advanced Options Menu screen.

To access the advanced options menu:

1. Reboot the computer (make sure all users are logged off before doing this).
2. Press F8 as soon as the computer boots.
3. Select the option you want to use (see Figure 16-12).
4. Highlight Microsoft Windows 2000 Server as the operating system option, and press Enter (make sure the option you selected in Step 3 is displayed at the bottom of the screen; if it is not, press F8 to return to the Advanced Options Menu).

Table 16-5 Advanced Menu Options

Booting Option	Description
Safe Mode	System boots using the minimum configuration of devices and drivers, and does not have network connectivity
Safe Mode with Networking	System boots using the minimum configuration of devices and drivers, and does have network connectivity
Safe Mode with Command Prompt	System boots into the command mode using the minimum configuration of devices and drivers, and does not have network connectivity
Enable Boot Logging	Used to create a record of devices and drivers that started, so you can check a log for points of failure—look for the log in the \Winnt folder with the name ntbtlog.txt
Enable VGA Mode	System boots using a generic VGA setting
Last Known Good Configuration	System boots using the last configuration before any changes were made and implemented in the Registry
Directory Services Restore Mode	Recreates the Active Directory service and the SYSVOL shared folder
Debugging Mode	Boots the system while transmitting debug data to be viewed at another computer over a serial connection, which can be used by Microsoft technicians to troubleshoot problems
Boot Normally	Boots the system without any special options
Return to OS Choices Menu	Returns to the regular operating system menu from which to select to boot into Windows 2000 (or another operating system on a dual-boot system)

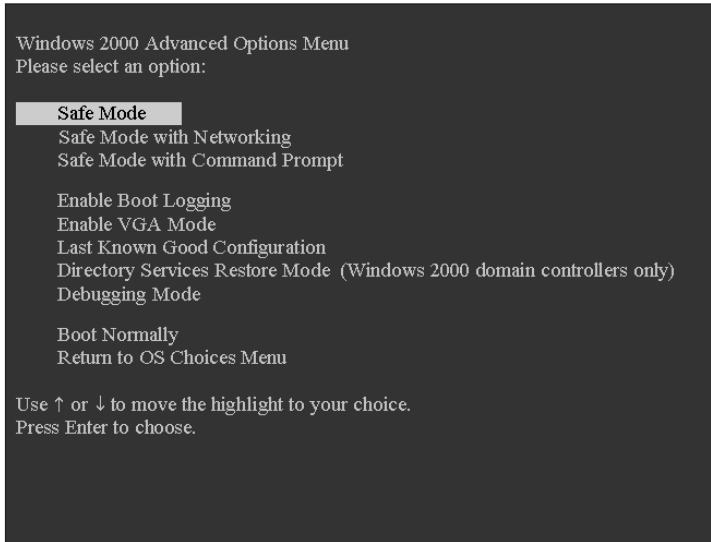


Figure 16-12 Advanced Options Menu for booting Windows 2000 server

Use the advanced option that is the most appropriate for the kind of problem you are troubleshooting. For example, if the problem is only that you have installed a new monitor driver and cannot use or see the display when you boot, select *Enable VGA Mode*. If the problem is related to the most recent software or configuration change you have made, such as installing an additional SCSI adapter or a new modem, boot using the *Last Known Good Configuration*. The **Last Known Good Configuration** is the Windows 2000 configuration that is stored in the Registry (HKEY_LOCAL_MACHINE\System\CurrentControlSet) and that is the configuration in effect prior to making a system, driver, or configuration change since the last time the computer was booted. For those times when you are not sure why the system is having problems, or you have installed multiple new drivers or several new software programs, use the *Safe Mode* or the *Safe Mode with Networking* option so that you can access the Windows 2000 desktop to work on the problem (try Hands-on Project 16-7 to practice booting into safe mode).

If you use safe mode, but are unable to troubleshoot the problem, or a failed driver message is displayed during the boot process, use the *Enable Boot Logging* option so that you can create a log that you can check later for problems. For example, you might boot so that the log is created, and then boot again into safe mode so that you can view the contents of the log.

The *Safe Mode with Command Prompt* option is particularly useful when you can solve a problem by executing a command, such as by running *chkdsk* to repair damaged files (see Chapter 7) or by running *sfc* (System File Checker, see Chapter 6) to locate critical system files that have been overwritten and then restore them.

If you have the Active Directory installed and suspect that it is damaged, or that the **SYSVOL** shared volumes (see the following Note) are corrupted, use the *Directory Services Restore Mode* to restore damaged files and folders.



When you set up the Active Directory, a domain controller is automatically set up with the SYSVOL shared volume, which contains publicly available files that users and DCs need for domain access. The SYSVOL shared folder exists on all DCs, and when the contents change on one DC, the change is replicated to all DCs.

Using the Emergency Repair Disk to Solve a Boot Problem

If rebooting does not work and you cannot solve the problem using the advanced menu options, then an alternative is to use the emergency repair disk (see Chapter 5), which can be used to restore key system and boot sector files. When started, the disk will take you through the repair steps, according to the type of problem it detects. To use the emergency repair disk, follow these steps:

1. Power off the computer.
2. If your computer supports booting from the Windows 2000 Server CD-ROM, boot from it. If not, insert the Windows 2000 floppy disk labeled Setup Disk 1 and boot from it (note that you must set the boot order in the BIOS, as explained in Chapter 5).
3. Power on the computer, enabling it to boot from the CD-ROM or floppy disk. If you boot from the floppy disk, follow the instructions to insert Setup Disk 2.
4. On the Welcome to Setup screen, press R for repair (see Figure 16-13).
5. On the next screen, press R again to use the emergency repair disk to perform the recovery (see Figure 16-14). Also note that there is an option to start the recovery console by pressing C (the recovery console is discussed in the next section).
6. Insert the emergency repair disk.



Figure 16-13 Accessing the repair option

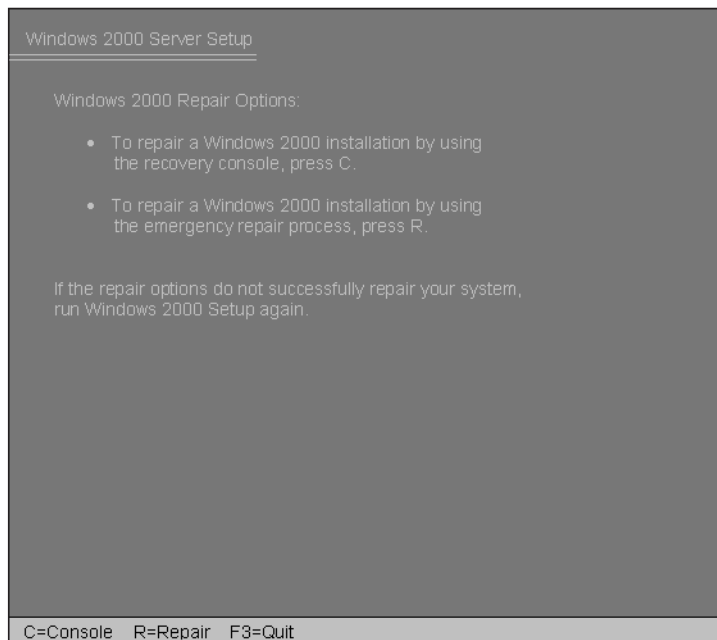


Figure 16-14 Repair options

7. There are two options that you can follow: one is to press M so that you can choose from a manual list of repair options, and the other is to press F to perform all repair options. If you select the manual option, you can select any or all of the following: inspect startup environment, verify Windows 2000 system files, and inspect boot sector. If you select F, then all of these functions are performed.
8. After you make your selection, follow the instructions on the screen to repair the problem.
9. Reboot the computer.

For example, you might use the emergency repair disk to repair the Master Boot Record by selecting the option to inspect the boot sector. Or you can repair Windows 2000 system files by choosing that selection. If you're not sure what is causing the problem, use the F option to perform all repair functions.



This is the time when keeping your emergency repair disk updated with every significant change on the server really pays off. Also, remember that you can back up Registry data onto the emergency repair disk if you check the box to back up the Registry when you create the disk. To make an emergency repair disk, format a floppy disk, insert it, click Start, point to Programs, point to Accessories, point to System tools, click Backup, and click emergency repair disk. Select the option to back up the Registry, and click OK.

Troubleshooting by Using the Recovery Console

In some situations, you may not be able to boot the computer into safe mode or restore a critical system file by using the emergency repair disk. The **recovery console** enables you to boot into the Windows 2000 Server command line so that you can repair a disk problem or copy a critical file back to the server. Another reason for using the recovery console is to start a service or to format a drive.



In Windows NT Server, server administrators sometimes created MS-DOS, Windows 95, or Windows 98 startup disks so that they could boot the system from Drive A using one of these operating systems, and then execute command-line utilities to troubleshoot problems, for example to format a disk. The recovery console makes creating this type of disk less important, because it provides a better way to access Windows 2000 Server files and repair utilities directly from Windows 2000 Server.

There are two ways to start the recovery console: (1) start it from the Microsoft Windows 2000 Server CD-ROM or installation disks, or (2) install the recovery console as a program that can be run when Windows 2000 Server is booted. To start the recovery console from the Microsoft Windows 2000 Server CD-ROM or installation disks:

1. Power off the computer.
2. Boot from the Windows 2000 Server CD-ROM, if your computer supports this boot option; otherwise, boot from the floppy disk labeled Setup Disk 1. If you boot from the floppy disk, follow the instructions to insert Setup Disk 2.

3. Press R for repair on the Welcome to Setup screen (refer to Figure 16-13).
4. On the next screen, press C to start the recovery console (refer to Figure 16-14).
5. After the recovery console is started, and if there are two or more drives containing \Winnt folders, the tool will ask which version you want to select. Or, if only one option is displayed, enter 1 to select it. Press Enter.
6. Enter the Administrator account password and press Enter.

The recovery console places you directly into the \Winnt folder, from which you can work in a character mode using command-line commands. To determine what commands are available, type *help* and then press Enter. The commands that you can use are:

- | | | | |
|----------|------------|-----------|--------------|
| ■ attrib | ■ delete | ■ fixmbr | ■ more |
| ■ batch | ■ dir | ■ format | ■ rd |
| ■ cd | ■ disable | ■ help | ■ ren |
| ■ chdir | ■ diskpart | ■ listsvc | ■ rename |
| ■ chkdsk | ■ enable | ■ logon | ■ rmdir |
| ■ cls | ■ exit | ■ map | ■ systemroot |
| ■ copy | ■ expand | ■ md | ■ type |
| ■ del | ■ fixboot | ■ mkdir | |

You can find information about the purpose and syntax of these commands by typing *help* and then the command, for example by typing *help attrib* and then pressing Enter. Use any of these commands to repair a problem. For instance, if you believe that the boot sector is corrupted on the system boot partition, use the *fixboot* command to fix it. Use the *fixmbr* utility to fix a corrupted Master Boot Record. Try Hands-on Project 16-8 to practice using the recovery console. Tables 16-6 and 16-7 provide some tips for fixing boot problems and responding to Stop error messages. A Stop message is an error message displayed when the server experiences a serious problem and then stops functioning.



Type *exit* and press Enter when you are ready to leave the recovery console and reboot into Windows 2000 Server.

Table 16-6 Troubleshooting Boot Problems

Boot Problem	Solutions
<p>A message appears when the system is booting, such as one of the following: Inaccessible Boot Device, Invalid Partition Table, Hard Disk Error, Hard Disk Absent or Failed.</p>	<ol style="list-style-type: none"> 1. The boot sector on the NTFS partition is corrupted, or the hard drive is damaged. This may be caused by a virus, a corrupt partition table, a BIOS setting change, or a corrupted disk. Check the BIOS setup to make certain it is correct. Correct any improper settings (also make sure the CMOS battery is working). 2. If there are no BIOS problems, boot the system using the recovery console. Insert a virus scanner in drive A and attempt to scan the hard disk for viruses. If a virus is found, remove it. Whether or not a virus is found, reboot so you can use the emergency repair disk to replace corrupted files. 3. If the disk cannot be accessed, determine if the problem is the hard disk, disk controller, or a SCSI adapter, and replace the defective part (make sure to check that a SCSI adapter is properly terminated). If the hard disk must be replaced, reinstall the operating system.
<p>The system hangs when booting.</p>	<ol style="list-style-type: none"> 1. Power the computer off and on to reboot. Try rebooting a couple of times. 2. If rebooting does not work, check the BIOS settings to be sure that they have not changed and that the CMOS battery is working. If many of the BIOS settings are incorrect, replace the battery and restore the proper settings. 3. Boot up so you can use the emergency repair disk, having it check the boot sector, startup, and system files. 4. For an SMP computer, the Hal.dll file may be corrupted. Boot up so you can use the recovery console to reinstall the Hal.dll from the manufacturer's disk.
<p>You see the message that there is a nonsystem disk or disk error.</p>	<ol style="list-style-type: none"> 1. Remove any disks from drive A or the CD-ROM drive and reboot. 2. If Step 1 does not work, boot using the emergency repair disk to reinstall the Boot.ini file, and other system files which may be corrupted on the system drive. 3. Boot so that you can access the recovery console and run <i>fixboot</i>.

Table 16-6 Troubleshooting Boot Problems (continued)

Boot Problem	Solutions
Changes were made to the system configuration when last logged on, and now the computer will not boot.	Stop the boot process immediately, reboot, press F8 and use the Last Known Good Configuration option on the advanced menu options screen. Once logged on, check the configuration and fix any problems, such as a bad or removed device driver.
The screen display goes blank or is jumbled as the computer begins booting into Windows 2000.	<ol style="list-style-type: none"> 1. Immediately stop the boot process. Restart the computer, accessing the BIOS Setup before starting Windows 2000. Check the video BIOS setup to make sure it is correct, and restore any settings that are changed. Reboot the computer. 2. If there are no BIOS problems, reboot using the Enable VGA Mode option from the advanced menu options. Once logged on, check and reinstall the display driver.
A driver is missing, but you are not sure which one, or the operating system is having trouble recognizing all hardware components on the computer when it boots.	Boot using safe mode and watch for a problem as the drivers are loaded, or boot using the Enable Boot Logging option from the advanced menu options and examine the \Winnt\ntbtlog.txt file.

Table 16-7 Troubleshooting Boot Problems Associated with Stop Messages

Stop Message*	Solutions
0x00000023 and the message Fat_File_System or NTFS_File_System	<ol style="list-style-type: none"> 1. Boot into safe mode or the recovery console and run <i>chkdsk</i> to repair any damaged files. 2. If you have recently installed a virus scanner or a disk defragmenter that is not from Microsoft or compatible with Windows 2000 Server, boot into safe mode or using Last Known Good Configuration and remove that software.
0x0000001E and the message Kmode_Exception_Not_Handled	<ol style="list-style-type: none"> 1. If you have recently installed a new video system and associated drivers, remove the new hardware, and reboot into safe mode to remove the new drivers (or boot using Enable VGA Mode). Do the same if you have installed any new drivers. 2. Verify the video setup in the computer's BIOS, or install any updated BIOS software offered by the computer vendor. 3. Reboot using safe mode or the recovery console and make sure that you are not out of disk space.
0x000000B4 and the message Video_Driver_Init_Failure	If you have recently installed a new video system and associated drivers, remove the new hardware, and reboot into safe mode to remove the new drivers (or boot using Enable VGA Mode).

Table 16-7 Troubleshooting Boot Problems Associated with Stop Messages (continued)

Stop Message*	Solutions
0x0000007B and the message Inaccessible_Boot_Device	<ol style="list-style-type: none"> 1. Boot into safe mode and check for a virus. 2. Boot into the recovery console and restore the Master Boot Record, using the <i>fixmbr</i> command. 3. Boot into the recovery console and run <i>chkdsk</i> to repair any damaged files. 4. Use the emergency repair disk and the F option to repair critical files.
0x0000002E and the message Data_Bus_Error or 0x0000007F and the message Unexpected_Kernel_Mode_Trap	Boot using the recovery console and run memory test software, such as diagnostics that come with your computer or from a memory vendor, and replace any defective memory.
0x0000000A and the message IRQL_Not_Less_Or_Equal	Suspect a hardware resource conflict caused by a new device or card you have added. If you can boot using safe mode, check the system log. If you cannot boot into safe mode, remove the new device or devices and boot using Last Known Good Configuration.
0x00000058 and the message Ftdisk_Internal_Error	Suspect that the main volume in a mirrored set has failed. Boot using the secondary volume, and use the Disk Management tool to attempt to repair the main volume and resynchronize it with the secondary volume. If you cannot repair the volume, use the Disk Management tool to break the mirrored set, replace the damaged disk, and then recreate the mirrored set.
0x000000BE and the message Attempted_Write_to_Readonly_Memory	Boot using the Enable Boot Logging option, and then boot again into safe mode (or the recovery console) so you can examine the <code>\Winnt\ntbtlog.txt</code> log for a driver that did not start or that is causing problems; then, reinstall or replace the driver using safe mode or by copying it into the system using the recovery console.

*For more information, see the Microsoft Help documentation entitled *Troubleshooting Specific Stop Messages*.

You can install the recovery console so that it is listed as an option along with the installed operating systems displayed in character-based mode just after you boot the server—eliminating the need to use the Windows 2000 Server CD-ROM or installation disks to access the recovery console. To install the recovery console, for example from CD-ROM drive D, insert the Windows 2000 Server CD-ROM, click Start, click Run, enter `D:\i386\winnt32.exe /cmdcons`, click OK, and click OK again to the message that the recovery console will be installed. Follow any additional instructions to complete the installation. For example, you may see an option to

log on to the Internet and download the software from the Microsoft Web site instead of loading it from the CD-ROM. As a last step, click OK to the notice that the recovery console has been installed.



If the Registry is corrupted, you can copy a version back while you are in the recovery console. Two copies of the Registry are kept in the `\Winnt` folder. One copy is located in the `\Winnt\repair` folder, which is the version of the Registry as it existed when you first installed Windows 2000 Server. A second copy is located in the `\Winnt\repair\regback` folder, which is created and updated each time you back up the system state data, a process described in the next section.

BACKING UP AND RESTORING SYSTEM STATE DATA

To protect against a disaster and to provide a way to recover system information, regularly back up the Windows 2000 Server system state data. In Windows 2000 Server, the system state data consists of several critical elements:

- System and boot files
- Active Directory
- SYSVOL folder (when the Active Directory is installed)
- Registry
- COM+ Class Registration information
- DNS zones (when DNS is installed)
- Certificate information (when certificate services are installed)
- Server cluster data (when server clustering is used)

All of the system state data is backed up as a group because many of these entities are inter-related. To back up the system state data, insert the backup medium, click Start, point to Programs, point to Accessories, point to System Tools, and click Backup. Next, click the Backup tab, click the drive you want to back up that contains the system state data, click the System State box under My Computer, and click Start Backup (see Figure 16-15). Each time you back up this information, for example to tape, a duplicate copy is also created in `\Winnt\repair\regback`.

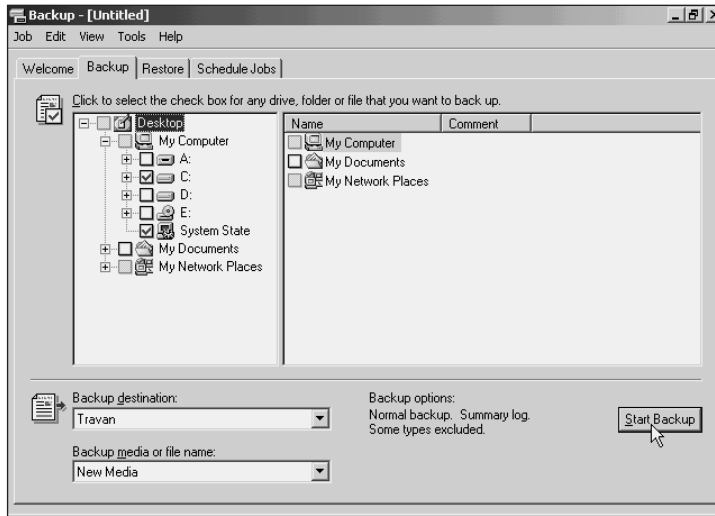


Figure 16-15 Backing up system state data



When you back up the system state data, keep in mind that you can only back it up from the local computer, which means that the backup medium, such as a tape drive, must be physically attached to that computer.

When you back up the system state data, also make sure you are backing up the protected system files, which are the startup system files needed by Windows 2000 Server. These files include:

- *Ntldr*, which initiates the startup process, operating system selection, and hardware detection
- *Bootsect.dos*, which is used for dual-boot systems
- *Boot.ini*, which is used by Ntldr to obtain startup information, such as which operating systems are available and their location
- *Ntdetect.com*, which detects the computer's hardware
- *Ntbootdd.sys*, which is a driver for SCSI adapters, if present
- *Ntoskrnl.exe*, which is the Windows 2000 Server kernel
- *Hal.dll*, which is the hardware abstraction layer

All of these files are located in the root of the system partition, except *Ntoskrnl.exe* and *Hal.dll*, which are in the `\Winnt\system32` folder. To ensure that the protected system files are backed up, make sure that the System State data is selected to be backed up before you click the Start Backup button. When you see the Advanced Backup Options dialog box before the backup starts, click the Advanced tab and then make sure that *Automatically backup System Protected Files with the System State* is checkmarked.

If you need to restore the system state data, remember that all of the data must be restored, not just selected portions, such as the Registry. To restore the system state data:

1. Open the Backup tool from the System Tools menu and click the Restore tab.
2. Insert the medium from which to perform the restore, such as a tape, and in the left pane, double-click the name of the medium from which to perform the restore, such as Travan or DAT (for a tape drive). In the right pane (or on the left pane under the medium) find the label of the backup that you want to restore and double-click it.
3. Click the drive that contains the system state data and also click the System State box.
4. In the Restore files to box, select the location to restore the files and folders.
5. Click the Start Restore button.
6. Click OK to start the restore.
7. Click Close and close the Backup tool.

RESTORING A FAILED SYSTEM VOLUME

If the drive containing the system volume fails, use the following steps to replace it and restore the information on it:

1. Replace the failed hardware.
2. Install Windows 2000 Server from the CD-ROM on the new drive.
3. Use the Backup utility to restore the system state data and all other data, using the most recent backup tapes.

If you are using only normal backups, then the restore simply involves using the most current normal backup tape or tapes. If you have designed the backups to combine normal plus differential or incremental backups, then there will be additional steps after restoring from the last normal backup. You will need to restore from the appropriate differential or incremental backups (see Chapter 7 for more information about backups and restores).



Sometimes you will need to turn to other resources to help you troubleshoot. There are many resources available through the Microsoft Web site (www.microsoft.com), such as the Knowledge Base, white papers, and TechNet information. A subscription to the Microsoft TechNet CDs is another reference source. On the Windows 2000 Server CD-ROM, check the \Support\Tools folder for additional tools you can use to manage your server, such as tools for managing the Active Directory and repairing disk problems. The Windows 2000 Resource Kit, which includes documentation not found in the manuals, may also be available in this folder or can be purchased from Microsoft.

CHAPTER SUMMARY

- ▣ Troubleshooting involves considerable strategy coupled with know-how gained by experience. As you start to troubleshoot server and network problems, develop a strategy that matches your particular equipment and organization. Complement the problem-solving techniques that you develop by enlisting users to help as partners and by understanding the business processes used in your organization.
- ▣ As you develop your problem-solving skills, learn to use the tools that are included with Windows 2000 Server, such as the Event Viewer, Network Monitor, System Monitor, Network and Dial-up Connections tool, Computer Management tool, System Security and Analysis tool, emergency repair disk, safe mode, recovery console, and Backup tool.
- ▣ An important part of the troubleshooting process is learning to use the right tool for the job. For instance, the Event Viewer is often a good starting place for locating and diagnosing a problem. If you keep the emergency repair disk updated and use the Backup tool to back up the system state data, both of these offer important help when there are boot problems or corrupted files. Safe mode provides a way to undo an improper configuration or software installation that has turned sour, and the recovery console gives you a way to start Windows 2000 directly in the command mode, to fix a problem.

Your growth as a server administrator is not complete without opportunities to grow through troubleshooting. Use these opportunities to help you better understand Windows 2000 Server and to develop patience and clear thinking in every aspect of managing and troubleshooting.

KEY TERMS

- application log** — An event log that records information about how software applications are performing.
- cyclic redundancy check (CRC)** — An error-checking technique used in network protocols to signal a communications problem.
- Directory Service log** — Records events that are associated with the Active Directory, such as updates to the Active Directory, events related to the Active Directory's database, replication events, and startup and shutdown events.
- DNS Server log** — An event log that provides information about events associated with the DNS Server, such as instances in which DNS information is updated, when there are problems with the DNS service, and when the DNS Server has started successfully after booting.
- dropped frames** — Frames that are discarded because they are improperly formed, for example failing to meet the appropriate packet size.
- event log** — One of several logs in which Windows 2000 Server records information about server events, such as errors, warnings, or informational events.
- File Replication Service log** — An event log that contains information about file replication events such as changes to file replication, when the service has started, and completed replication tasks.

Last Known Good Configuration — The Windows 2000 configuration that is stored in the Registry and that is the configuration in effect prior to making a system, driver, or configuration change since the last time the computer was booted.

recovery console — A recovery tool that enables you to access the Windows 2000 Server command line to perform recovery and troubleshooting operations. The recovery console can be added as a boot option, started from the Windows 2000 Server CD-ROM, or from the Windows 2000 Server floppy installation disks.

Run as / runas — A shortcut menu and command-line option that enables you to run a Windows 2000 program or utility from one account, such as Administrator, while logged on as another account.

safe mode — A boot mode that enables Windows 2000 Server to be booted using the most generic default settings—such as settings for the display, disk drives, and pointing device—and only those services needed to boot a basic configuration.

security log — An event log that records access and security information about logon accesses and file, folder, and system policy changes.

system log — An event log that records information about system-related events such as hardware errors, driver problems, and hard drive errors.

SYSVOL — A shared folder that is set up when the Active Directory is installed and that contains publicly available files that users and DCs need for domain access. SYSVOL folders are replicated among DCs.

REVIEW QUESTIONS

1. You have made several changes to the monitor display settings by using the Display icon in the Control Panel. When you reboot into the Windows 2000 Server desktop after making these changes, the monitor just flickers and you see nothing. Which of the following advanced boot options can you try next to enable you to boot so that you can view the desktop and change the settings back?
 - a. Safe Mode
 - b. Enable VGA Mode
 - c. Last Known Good Configuration
 - d. all of the above
 - e. none of the above
 - f. only a and b
2. Several users are having problems accessing a newly created shared folder. The problem is that your network has several hundred groups, and it will be time-consuming for you to examine the permissions associated with each group in relation to group members. What is another and better alternative for troubleshooting this problem?
 - a. Give all of those users System Operator privileges to save you time.
 - b. Ask one of those users to share the information from her computer, instead of sharing it from the server.

- c. Make sure that the shared folder does not have any files that were copied from another folder, because that can cause the entire folder to inherit permissions brought in by copied files.
 - d. Audit successful and failed access to that folder.
- 3. You are consulting at a new site and do not know the IP address of a particular Windows 2000 server that you have accessed using an account with Administrator privileges. Which of the following tools enables you to quickly determine the IP address and subnet mask at the same time?
 - a. winipcfg
 - b. net user
 - c. ipconfig
 - d. all of the above
 - e. only a and b
 - f. only b and c
- 4. You need to troubleshoot a boot problem on a Windows 2000 server, and you want to make sure that you do not have network connectivity while you are troubleshooting (to keep users from logging on). Which of the following advanced boot modes can you use?
 - a. Safe Mode with Command Prompt
 - b. Enable VGA Mode
 - c. Safe Mode
 - d. all of the above
 - e. none of the above
 - f. only a and b
 - g. only a and c
- 5. You walk into the computer room one morning and notice that there is a message at the Windows 2000 Server console that the application log is full. Which of the following might be true?
 - a. The application log needs to be set to a larger size.
 - b. The application log is set to *Do not overwrite events*.
 - c. The application log is left at the default setting to record up to 100 events as a maximum.
 - d. all of the above
 - e. only a and b
 - f. only a and c

6. Yesterday, you installed RIS but were interrupted shortly after the installation because a problem came up on a server. Today you are trying to run RIS, but it does not work. How can you go back and check to see if you configured it?
 - a. Check the Control Panel for the RIS icon.
 - b. Look in the Add/Remove Programs window by checking the Add/Remove Windows Components option.
 - c. Check in the Computer Management tool, using the Components option in the tree.
 - d. Look for a RIS connection icon in the Network and Dial-up Connections tool.
7. Which of the following can you use to access the emergency repair disk in order to fix a boot problem?
 - a. recovery console
 - b. Windows 2000 Server CD-ROM or setup disks
 - c. Computer Management tool
 - d. System Monitor
8. Your diagnosis of a problem that prevents your server from booting is that the Master Boot Record is corrupted. Which of the following tools enable(s) you to access the server so that you can repair it?
 - a. recovery console
 - b. safe mode
 - c. emergency repair disk
 - d. all of the above
 - e. only a and b
 - f. only a and c
9. Which of the following can prove to be a valuable tool in diagnosing network and server problems?
 - a. training users to provide information about problems
 - b. creating a network diagram
 - c. keeping a database of problems and their resolution
 - d. all of the above
 - e. only a and c
 - f. only b and c
10. The financial auditors at your organization have requested that you audit all successful and failed accesses to the vouchers and payroll files. Where do you look to view the audit results?
 - a. Directory Service log
 - b. system log

- c. security log
 - d. All of the above will contain that information.
 - e. only a and c
 - f. only b and c
11. Which of the following tools can you use to troubleshoot a hardware resource conflict between a NIC and the floppy disk drive?
- a. Device Manager
 - b. Services tool
 - c. Computer Management tool using the System Information option in the tree
 - d. all of the above
 - e. none of the above
 - f. only a and b
 - g. only a and c
12. One of your users has just gotten a new computer and connected it to the network. She has sent only one document to the printer, which printed a couple of strange characters per page, on 30 pages. Only this user has reported the problem. Which of the following might you do at this point?
- a. Press the reset button on the printer.
 - b. Reinstall the printer driver on her computer, installing the version from the server to make sure it is compatible with the network and that network printer.
 - c. Use a different printer cable between the printer and the server.
 - d. all of the above
 - e. only a and b
 - f. only a and c
13. While you are logged on to a Windows 2000 Web server, you receive a call from a user who cannot connect to the Internet. How can you quickly test the Internet connection from the Web server?
- a. Use the Computer Manager to send a test set of frames onto the full network from the server.
 - b. Ping a computer at a distant location on the Internet.
 - c. Use the recovery console to send a Net Internet command.
 - d. You cannot test an Internet connection from a Windows 2000 server.

14. Your new assistant has set up the NIC and TCP/IP for Windows 2000 Server on a computer, but it is not communicating on the network. You decide to verify the IP address and subnet mask. Which of the following tools can you use?
 - a. winipcfg
 - b. FTP
 - c. Network and Dial-up Connections
 - d. all of the above
 - e. only a and b
 - f. only a and c
15. The computer committee on your campus is very concerned about security. One of the members has heard about the System Security and Analysis tool and insists that you should be using it to block intruders, because she claims that it can detect accounts that are intruding and then automatically disable those accounts. What is your response?
 - a. This is an appropriate tool for the functions she has described.
 - b. This tool cannot fulfill her claims, but it can be used to configure security and to later analyze security.
 - c. This tool only automatically blocks the accounts that you specify within the tool.
 - d. This tool is only capable of analyzing file and folder security.
16. One of your disk drives is experiencing problems and has corrupted some files in the \Winnt folder. Sometimes the server will boot and sometimes it will not. Your goal is to repair the files to see if that will fix the problem. Which of the following tools offers the best hope in this situation?
 - a. Use the recovery console and run *chkdsk*.
 - b. Use the Computer Management tool and defragment the disk.
 - c. Use the Event Viewer to identify and repair each damaged file.
 - d. Use the emergency repair disk to restore SYSVOL.
17. Which of the following is(are) system state data on a Windows 2000 server that has the Active Directory installed?
 - a. SYSVOL folder
 - b. Registry
 - c. system files
 - d. all of the above
 - e. none of the above
 - f. only a and b
 - g. only a and c

18. You regularly back up system state data on your server. Now you need to restore it, but the tape on which you backed it up is damaged and cannot be read. What is your best alternative for restoring this data?
 - a. You have no good alternatives, except to reinstall Windows 2000 Server.
 - b. Recover the data by using the ntbt.log in the root of the server.
 - c. Recover the data using the \Winnt\repair\regback folder data.
 - d. Recover the data from the Netlogon shared folder.
19. Your assistant is working on a Windows 2000 server updating server DNS records and has several other windows open. His account only has limited privileges, one of which is to access DNS to work on these updates. A network slowdown has been reported to you, and you want to start System Monitor to track several objects for a few minutes. Can you run System Monitor as Administrator without logging off your assistant's account?
 - a. Yes, by using the Run as utility.
 - b. Yes, by spawning a System Monitor process as a subprocess in Control Panel.
 - c. Yes, by using the MMC instead of the Administrative Tools menu.
 - d. No, you have no choice but to log off your assistant.
20. Your Windows 2000 server is having trouble booting, and you suspect that the problem is related to a driver or service that is not properly starting. How can you track each of the startup actions of the server so that you can later go back and review each one for problems?
 - a. Use the Net Log command from the recovery console.
 - b. Select Enable Boot Logging from the advanced menu options when you boot.
 - c. Select the Debugging Mode from the advanced menu options when you boot.
 - d. Enable Full System Logging as a group policy and then reboot the server.
21. Which of the following might be part of your problem-solving strategy?
 - a. Reboot the server once a day to prevent problems and reset all registers.
 - b. Regularly check the event logs.
 - c. Look for the simple solutions first.
 - d. all of the above
 - e. only a and b
 - f. only b and c
22. The system log contains hundreds of entries, but you only want to look at error events associated with the Workstation service. How is this possible?
 - a. Create a trap.
 - b. Turn off recording of the information and warning events.
 - c. Set up a filter.
 - d. Print out the log so that it is easier to read.

23. You want to periodically monitor for intruders. Which of the following tools can you use?
- System Monitor using the Server object
 - Network Monitor using the Graph pane
 - Periodically boot into the Safe Mode with Networking option.
 - all of the above
 - only a and b
 - only a and c
24. Server users have called to say that they cannot reach a Windows 2000 server that is configured for TCP/IP. You know that the NIC on that server had some problems earlier this morning. As a quick first step in diagnosing the problem, you decide to see if the server is transmitting on the network. Which of the following tools enables you to do that?
- ipconfig
 - Active Directory Computers and Users
 - System Monitor Job Object
 - netstat
25. Which of the following tools keeps a security-related database and enables you to examine existing security settings in one place?
- Active Directory Trusts and Domains tool
 - System Security and Analysis tool
 - Active Directory Users and Computers tool
 - System Monitor Security object

HANDS-ON PROJECTS



Project 16-1

This project gives you the opportunity to use the Event Viewer and to build a filter.

To use Event Viewer and configure a filter:

- Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Event Viewer**.
- If no logs appear in the tree, double-click **Event Viewer (local)**.
- What logs are available? Click each log to view its contents, and record your observations in your lab journal or in a word-processed document.
- Click **System Log** and briefly scroll through its contents.
- Are there any errors reported? If so, look at one or two of the errors.
- Right-click **System Log** and click **Properties**.

7. Look first at the General tab. Where is the system log stored? What is the maximum size for the log, and what will happen when the maximum size is reached? Record your observations.
8. Click the **Filter** tab.
9. Click the list arrow in the **Event source** box and scroll through the options. Record some of the options that you recognize. Select **Netlogon** so that you only view events associated with logon activity.
10. In the Event types section, remove the check marks from all events except Error. Are any event type options deactivated?
11. Notice the other parameters that you can set for a filter, and record your observations.
12. Click **OK**.
13. How does using the filter change what you view in the system log? Does this mean that the events you viewed before creating the filter are deleted, or simply not displayed?
14. Close Event Viewer.



Project 16-2

In this project, you practice using the Computer Management tool to troubleshoot a hardware resource conflict.

To troubleshoot the resource conflict:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Computer Management**.
2. Double-click **System Tools**, if the objects under it are not displayed. What tools are available under System Tools?
3. Double-click **System Information**, and then double-click **Hardware Resources** in the tree. What objects are displayed under this option? Record your observations.
4. Double-click **Conflicts/Sharing** in the tree.
5. Are any conflicts displayed? How would you solve a conflict? Are there some types of conflicts that do not represent a problem?
6. Leave the Computer Management tool open for the next assignment.



Project 16-3

In this project, you use the Device Manager to verify that a NIC is working, and you practice looking for a resource conflict at the NIC.

To troubleshoot a NIC using the Device Manager:

1. Make sure that the Computer Management tool is open, and if not, open it.
2. Double-click **Device Manager** in the tree.
3. Double-click **Network adapters**, and then double-click a network adapter that is listed.

4. What information is displayed that enables you to verify that the adapter is working properly? Record your observations.
5. Click the **Resources** tab. How can you determine if there is a resource conflict? How would you resolve a conflict if one existed?
6. Close the NIC properties dialog box, and then close the Computer Management tool.



Project 16-4

In this activity, you have an opportunity to use *nbtstat* to view computers on the network and then *netstat* to view all connections. You can use a computer running Windows 2000 Server or Windows 2000 Professional to complete this assignment.

To test TCP/IP connectivity using *nbtstat* and *netstat*:

1. Click **Start**, point to **Programs**, point to **Accessories**, and click **Command Prompt**.
2. At the command prompt, enter **nbtstat -n** and press **Enter**. What information is displayed? Record your observations.
3. Next, type **nbtstat -s** and press **Enter**. What information is displayed by this command? Record your observations.
4. Now type **netstat -a** at the command prompt. What information is produced by this command? Note your observations.
5. How can you use the *ipconfig* command to verify your own TCP/IP connection? What is the purpose of the *ping* command? Try both of these commands.
6. Close the Command Prompt window.



Project 16-5

In this project, you practice taking ownership of a folder (even though the folder in this example is already owned by the Administrators group). You will use the \Winnt folder, which should be on an NTFS-formatted disk.

To take ownership of a folder:

1. Double-click **My Computer**, then double-click Local Disk **C:** or whichever drive contains the \Winnt folder.
2. Right-click **Winnt** and click **Properties**.
3. Click the **Security** tab and then click the **Advanced** button.
4. Click the **Owner** tab. What users and groups are listed as possible owners?
5. In the *Change owner to* box, click **Administrators**.
6. Click **OK** and click **OK** again.
7. Close My Computer.



Project 16-6

In this project, you practice using the Security Configuration and Analysis tool to analyze security. Before starting, ask your instructor which database to use in the project.

To analyze security:

1. Click **Start**, click **Run**, and type **mmc** in the Open box. Click **OK**.
2. Maximize both console windows, if they are not already maximized.
3. Click the **Console** menu, and click **Add/Remove Snap-in**.
4. Click the **Add** button and then double-click **Security Configuration and Analysis**.
5. Click **Close** and then **OK**.
6. Right-click **Security Configuration and Analysis** in the tree, and click **Open Database**. What database options are available from which to select? Why might there be more than one database shown?
7. Click the database specified by your instructor, and then click **Open**. What is now displayed in the right pane?
8. Right-click **Security Configuration and Analysis** again, and then click **Analyze Computer Now**.
9. Where is the error log file written? Can you change its location? Record your observations. Click **OK**.
10. What information is displayed next, as the tool performs the analysis?
11. If the log file contents are not displayed in the right-hand pane, right-click **Security Configuration and Analysis** and place a checkmark in front of **View Log File**. Or, if View Log File is already checked, remove the check, right-click **Security Configuration and Analysis** again and checkmark **View Log File**.
12. Scroll through the log file in the right-hand pane. What kind of information is analyzed?
13. How can you view information about current security settings?
14. Close the MMC, and click **No** if you are asked if you want to save the console settings.



Project 16-7

This project gives you an opportunity to practice booting into safe mode.

To boot into safe mode:

1. Make sure all users are logged off Windows 2000 Server. What tool would you use to check this?
2. Reboot the computer (click **Start**, click **Shut Down**, and select the **Restart** option—or power off the server and reboot).
3. Press **F8** as soon as the computer boots.
4. What are the options that you see on the screen? Which option would you use to boot to fix a monitor driver problem? Which one would you use to run chkdsk?
5. Select **Safe Mode** and press **Enter**.

6. What information is displayed at the bottom of the screen?
7. Highlight **Microsoft Windows 2000 Server** as the operating system option, and press **Enter**.
8. What information is displayed as the system boots? How might this information prove helpful in troubleshooting a problem?
9. Press **Ctrl+Alt+Delete** and enter an account name and password.
10. Click **OK** to the warning message that you are in safe mode.
11. How is the Windows 2000 Server desktop display different in safe mode from when you boot normally?
12. Record your observations about safe mode, and then reboot the computer.



Project 16-8

In this project, you practice using the recovery console. You will need the Windows 2000 Server CD-ROM or the Windows 2000 Server floppy installation disks. Also, obtain the Administrator account password from your instructor.

To boot into the recovery console:

1. If the server is already booted, make sure all users are logged off Windows 2000 Server. Insert the Windows 2000 Server CD-ROM or Setup Disk 1, and reboot the computer (click Start, click **Shutdown**, and select the **Restart** option—or power off the server and reboot). If your computer supports booting from the Windows 2000 Server CD-ROM, boot from it. If not, use the Windows 2000 floppy disk labeled Setup Disk 1 and boot from it (note that you may need to set the boot order in the BIOS, as explained in Chapter 5). If you boot from floppy disk, follow the instructions to insert Setup Disk 2.
2. On the Welcome to Setup screen, press **R** for repair (refer to Figure 16-13).
3. On the next screen, press **C** for recovery console (refer to Figure 16-14).
4. Select the drive containing the \Winnt folder you want to access, for example by typing **1** to access \Winnt on drive C. Press **Enter**.
5. Type the Administrator account password, and press **Enter**. What is displayed on the screen?
6. Type **help** and press **Enter**. What information do you see? Can you run chkdsk (the check disk utility)? Press the **Spacebar** to continue scrolling the options.
7. Type **help diskpart**. What can you do with this utility? What utility would you use to repair the Master Boot Record?
8. Record your observations. Type **exit** and press **Enter** to leave the recovery console and reboot.

CASE PROJECT



Aspen Consulting Project: Troubleshooting

Haberdashers is a clothing manufacturer for women and men that specializes in trendy fashions. The main offices of the company are in a building that is fully networked and houses eight Windows 2000 servers. The management, customer service, marketing, planning, and financial services groups are located in the main offices. All of the servers run 24 hours a day, 7 days a week, because the customer service group always has people available to take orders by Web server and by telephone. Customer Service also works to coordinate shipments with the inventory and distribution groups, who are in five locations in Canada and the United States. The server administrator with the most troubleshooting experience has just resigned to take another job, and Haberdashers has hired you as a resident consultant until you can train another server administrator in troubleshooting.

1. When you first start training the server administrator who will be the main troubleshooter, what recommendations do you have for developing a troubleshooting strategy?
2. While you are training the server administrator, one of the servers suddenly crashes. Where would you look first for a clue about what happened, and how would you explain to the administrator the steps and tools you would use?
3. The vice president in charge of the marketing group is working to launch a costly new marketing campaign and already is experiencing a lot of pressure. She calls you because some of her staff cannot access several new folders that have been set up for them. Also, it appears that someone has obtained information from a top-secret folder and provided it to a competing company. What tools and techniques can you use to address these problems as quickly as possible?
4. As a result of a sudden power surge transferred by a grounding problem in the network cable, the server that has customer service data seems to have several corrupted system files, a corrupted Registry, and intermittent problems booting. The administrator that you are training is on the scene first, and now reports that the server either displays a message that there is a nonsystem disk or it hangs while booting. What techniques and tools can you use to troubleshoot and solve this problem?
5. After you solve the booting problem, people report that the network printer attached to that server is now printing “weird” characters. How would you address this problem?
6. Once the problems in Assignments 4 and 5 are solved, your trainee asks about the function of system state data. Explain the purpose of this information and how it can be backed up and restored.

OPTIONAL CASE PROJECTS FOR TEAMS



Team Case One

Mark Arnez has observed that your firm is now responding to a large number of calls asking for help in using the recovery console. He asks you to form a team to document all of the commands that can be used from the recovery console and provide sample situations in which someone would use them.



Team Case Two

Another common problem area is TCP/IP connectivity. Mark Arnez asks your team to develop a flow chart that provides a summary of steps to take for different kinds of TCP/IP connectivity problems. In addition to the chart, he asks your team to list and briefly summarize the tools that can be used to solve those problems.